Abstract

Method and devices are directed to uniquely identifying content in a

5 highly distributed content delivery system such that an origin of unauthorized content use
may be more accurately determined. Content received from a content owner is
distributed to a persistent security database and a key manager, which manages
encryption and decryption keys for content that may be already encrypted. Decrypted
content is fingerprinted or watermarked by a fingerprinter / watermarker module such
10 that a recipient of content is identifiable, and saved in a separate database. Information
about fingerprinted / watermarked content may be reported back to content owner for
tracking purposes. A key wrap module wraps and attaches aggregator's encryption key
to the content before it is transmitted to downstream service operators or users.